Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/CN04/001592

International filing date: 31 December 2004 (31.12.2004)

Document type: Certified copy of priority document

Document details: Country/Office: CN
Number: 200310121630.6
Filing date: 31 December 2003 (31.12.2003)

Date of receipt at the International Bureau: 28 February 2005 (28.02.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

PCT/CN2004/001592

证　　明

本证明之附件是向本局提交的下列专利申请副本

申　请　日：　2003.12.31

申　请　号：　200310121630.6

申请类别：　发明

发明创造名称：　一种安全的网上支付系统及安全的网上支付认证方法

申　请　人：　中国银联股份有限公司

发明人或设计人：　彭桂林、康建明、危刚、姚加贤、王楠、张莉莉、梁建

中华人民共和国
国家知识产权局局长　王景川

2005 年 1 月 13 日

权 利 要 求 书 031372

1. 一种网上支付系统，包括如下组成部分：

客户，即消费者，需要从其帐户中向商户支付一定数量货币的一方，

客户支付帐户银行或其代理行，即可以确认帐户信息和执行扣款支付的一方，

商户，即服务或商品提供者，应该收取款项的一方，

商户收款帐户银行或其代理行，

支付平台，是负责处理来自网上的支付信息，并且认证客户和商户身份，确认交易真实有效的一个处理系统，

客户、商户和支付平台通过互联网连接，在支付平台的处理系统确认交易的合法性之后，支付平台发出支付请求，并在支付完成后将支付信息通知交易双方，即客户和商户，

支付平台一端联系客户和商户，在互联网上确认客户身份与商户身份，互联网上对客户身份认证是密码认证方式进行的，对商户身份认证是证书认证方式进行的，并确认交易与交易金额；一端联系支付帐户银行和收款银行，传送支付请求与扣款信息，

其特征在于：

支付平台中有客户信息数据库，包括客户真实身份和网上交易客户身份及其帐户基本信息，

在支付平台与客户之间还设有客户身份辅助认证系统，该辅助认证系统连接客户与支付平台，并且是非互联网连接方式，

支付平台在互联网上确认网上交易客户身份在客户信息数据库中有正确记录，即客户身份有效以后，根据收到的支付请求，生成一个授权码，并通过客户身份辅助认证系统传送该授权码给客户，客户在收到该授权码以后，在支付平台的相应页面上输入该授权码，支付平台在核实授权码无误后，确认客户身份通过验证，发送支付信息，并从银行获得返回的处理信息，并将该处理信息传送给客户与商户。

2．如权利要求 1 所述的网上支付系统，其特征在于：所述的客户身份辅助认证系统包括一个客户终端和一个转接系统，该客户终端在支付平台中有初始信息登记，该转接系统连接支付平台与客户终端，从支付平台接收信息并传送到客户终端。

3．如权利要求 2 所述的网上支付系统，其特征在于：所述的转接系统从支付平台接收的信息，包括授权码和交易信息。

4．如权利要求 1 所述的网上支付系统，其特征在于：所述的授权码是动态生成并且是有时效的，在时效范围以内输入到支付平台的相应页面，该授权码才能被认为是正确的，超出时间范围则被判断为无效的授权码。

5．如权利要求 1 或 2 所述的网上支付系统，其特征在于：所述的客户身份辅助认证系统的客户终端是专用设备，该专用设备在支付平台中有初始信息登记。

6．如权利要求 5 所述的网上支付系统，其特征在于：所述的客户终端是单独设置的由该支付平台提供的专用设备。

7．如权利要求 5 所述的网上支付系统，其特征在于：所述的客户终端是符合该支付平台标准的设备。

8．如权利要求 5 所述的网上支付系统，其特征在于：所述的客户终端是由该支付平台提供的专用转接卡设置在个人或家庭常见电子或电器设备中形成，如机顶盒、遥控器等。

9．如权利要求 1 或 2 所述的网上支付系统，其特征在于：所述的客户身份辅助认证系统的客户终端是非专用设备，如电话、手机、BP 机、PDA 等，该非专用设备作为客户终端使用前需要到支付平台或其指定地方进行初始信息登记。

10．如权利要求 2 所述的网上支付系统，其特征在于：所述的客户终端在该支付平台的初始信息登记可以是一个或多个客户终端的信息。

11．如权利要求 2 所述的网上支付系统，其特征在于：所述的接收授权码的客户终端可以不是该支付平台中有初始信息登记的客户终端。

12. 如权利要求 1 所述的网上支付系统，其特征在于：该系统在支付平台和银行之间还设有银行信息处理系统，该银行信息处理系统联系支付平台和支付帐户银行或其代理行和收款帐户银行或其代理行，支付平台发送支付请求给该银行信息处理系统，并从该系统获得支付请求的处理结果，扣款成功或拒绝支付。

13. 如权利要求 12 所述的网上支付系统，其特征在于：所述的支付平台和银行信息处理系统，是由不同机构提供的网络平台。

14. 如权利要求 12 所述的网上支付系统，其特征在于：所述的支付平台和银行信息处理系统，是由同一机构提供的网络平台。

15. 如权利要求 12 所述的网上支付系统，其特征在于：所述的银行信息处理系统，是由付款人帐户开户银行提供的网络平台。

16. 如权利要求 12 所述的网上支付系统，其特征在于：所述的银行信息处理系统，是由收款银行或其代理行提供的网络平台。

17. 如权利要求 13 所述的网上支付系统，其特征在于：所述的支付平台和银行信息处理系统，是由与交易无关的第三方提供的网络平台。

18. 如权利要求 1 或 12 所述的网上支付系统，其特征在与所述的支付平台中设有客户信息数据库，该数据库中包括客户信息和其对应的银行帐户信息，其中客户信息中的客户身份包括真实身份和网上交易身份，该网上交易身份可以是真实身份，或者是客户任意设定的身份。

19. 一种网上支付认证方法，包括对网上交易的双方，即客户和商户进行身份认证并确认其交易和交易金额，商户身份进行证书认证，客户身份进行密码认证，其特征在于对客户身份还进行动态的辅助认证。

20. 一种如权利要求 19 所述的网上支付认证方法，包含如下步骤：

客户网上浏览，发出交易请求，

商户接收交易请求，

客户发出支付请求，转入支付平台界面，

支付平台要求客户在互联网上输入网上支付密码进行客户身份认证，并核实该密码，

若密码不正确，则拒绝该交易请求，

若密码正确，则动态生成授权码，

支付平台通过客户身份辅助认证系统传送该授权码给客户，

客户在收到该授权码以后，在支付平台的相应页面上输入该授权码，

支付平台在核实授权码无误后，确认客户身份通过验证，发送支付请求，

其中，所述的客户身份辅助认证系统传送授权码给客户系通过非互联网途径传送。

21．一种如权利要求 20 所述的网上支付认证方法，其特征在与：所述的支付平台在核实授权码无误后，发送支付请求系发送到银行信息处理系统，由银行信息处理系统通知付款人开户银行执行扣款，并将处理结果返回给支付平台。

22．一种如权利要求 20 所述的网上支付认证方法，包含如下步骤：

1. 客户在商户网站选择商品并形成订单；
2. 客户选择身份辅助认证方式为手机短信认证方式，（建议，以区别于固话短信认证方式）
3. 客户进入到网上支付系统的支付平台界面，根据界面提示输入手机号码及网上支付密码；
4. 支付平台收到客户信息后对手机号及网上支付密码进行判断，若该手机信息已经有初始信息并且密码准确，则动态生成一个授权码；
5. 支付平台将该授权码发往短信中心；
6. 短信中心将收到的授权码发到客户手机上；
7. 客户收到短信，根据提示在支付网页上输入授权码；

8. 支付平台对授权码进行校验无误后，视为客户身份认证通过，进行下一步的支付程序。

23. 一种如权利要求 20 和 21 所述的网上支付认证方法，其特征在于所述的动态生成授权码同时还指定该授权码的有效时间，必须在指定的时间范围内输入正确的授权码。

24. 一种如权利要求 20 所述的网上支付认证方法，其特征在于所述的支付平台通过客户身份辅助认证系统传送授权码和交易信息给客户终端。

25. 一种如权利要求 20 所述的网上支付认证方法，其特征在于所述的支付平台通过客户身份辅助认证系统传送该授权码给客户，系传送到客户终端上。

26. 一种如权利要求 20 所述的网上支付认证方法，其特征在于所述的支付平台通过客户身份辅助认证系统传送授权码到客户终端，该客户终端是由客户指定的。

一种安全的网上支付系统及安全的网上支付认证方法

技术领域

本发明涉及一种安全的网上支付认证方法，以及应用了此方法的一种安全的网上支付系统。

背景技术

近年来，电子商务逐渐成为互联网经济发展的主要潮流，网上购物和支付逐渐成为一种方便的生活方式。电子商务的关键环节之一是支付结算体系，而网上支付则是电子商务最理想的支付方案。

目前主要的网上支付工具主要有银行卡、电子支票、电子钱包等，其中应用最广泛的支付工具是银行卡。

本发明的网上支付系统主要涉及使用银行卡作为支付工具通过互联网完成电子商务交易的付款方式。

网上支付的核心问题是安全问题。

电子商务必须在一个安全的环境下进行，包括以下三层含义：

1. 数据保密性

网上交易数据在传输过程中要保证不被截获、窃取而被非法使用。

2. 数据完整性

网上交易数据在传输过程中要保证数据没有改变、丢失而失真。

3. 主体真实性

网上交易的进行要保证参与交易的消费者就是合法的持卡人或银行帐户的拥有者，销售者就是合法的商户。

网上支付的面临的现实困难如下：

1. 交易数据的保密性和完整性

交易数据借助于 Internet 互联网传递，而互联网又是一个开放的网络，交易数据很容易被截获、窃取、改变，从而进行非法使用。

2. 交易主体的认证

传统的网上支付过程对持卡人基本上是不加认证的，消费者只须输入信用卡号和有效期就能顺利地完成一笔交易，由于卡号和有效期都是非机密信息，这就使得这些信息的盗取十分容易。信用卡网上支付欺诈案数量的大量上升就难以避免了。

为了解决上述问题，已经出现了多种安全认证方案，主要有以下一些技术手段：

1. SSL 加密机制（Secure Socket Layer）

SSL 是一种加密算法，是由 Netscape 首先发表的网络资料安全传输协定，其首要目的是在两个通信间提供秘密而可靠的连接。SSL 握手协议准许服务器端与客户端在开始传输数据前，能够通过特定的加密算法相互鉴别。SSL 的先进之处在于它是一个独立的应用协议，其它更高层协议能够建立在 SSL 协议上。

大部分的 Web Server 及 Browser 大多支持 SSL 的资料加密传输协定。因此，可以利用这个功能，将部分具有机密性质的网页设定在加密的传输模式，如此即可避免资料在网络上传送时被其他人窃听。 SSL 是利用公开密钥的加密技术（RSA）来作为客户端与主机端在传送机密资料时的加密通讯协定。目前，大部分的 Web Server 及 Browser 都广泛使用 SSL 技术。对消费者而言，SSL 已经解决了大部分的问题。但是，对电子商务而言问题并没有完全解决，因为 SSL 只做能到资料保密，厂商无法确定是谁填下了这份资料，即使这一点做到了，还有和银行清算的问题。

2. 安全电子交易规范 SET（Secure Electronic Transaction）

1996 年，MasterCard、Visa、American Express 国际信用卡组织与技术厂商 IBM 共同制定了 SET。SET 是一个完美的技术主义产物，对持卡人、商户、银行都有数字证书的认证。SET 运用了 RSA 安全的公钥加密技术，具有资料保密性、资料完整性、资料来源可辨识性及不可否认性，是用来保护消费者在 Internet 持卡付款交易安全中的标准。

SET 是由 Electronic Wallet（电子钱包）、Merchant Server（商店端

服务器）、Payment Gateway（支付平台）和 CA（Certification Authority，认证中心）组成的，它们构成了 Internet 上符合 SET 标准的信用卡授权交易。

SET 协议用在安全电子银行卡的支付系统中，使用客户端的浏览器，应用于从商业站点到商业银行中。网上银行使用已经存在的程序和设备通过确认信用卡，清算客户银行户头完成交易。SET 协议则通过隐藏信用卡号来保证整个支付过程的安全。所以，SET 必须保证信用卡持有者与银行在现存系统和网络上，能够保持持续的联系。SET 协议为在不同的系统中使用信用卡创建了一套完整的解决办法。可靠的身份验证使 SET 成为一个非常好的在线支付系统。它使交易中每个合法参与者能够拥有一个合理的身份，而对持卡者的身份验证是由银行来进行的。当然这其中还包括其它服务，比如：身份认证、客户服务等。这是建立另外一个可靠的客户连接的方法。同时可以方便在发生纠纷时进行仲裁。

利用证书进行认证需要在被认证对象的电脑上安装证书软件，这种方式用于认证商户是可行的，但当用于认证持卡人时，由于很多网上购物者并不使用固定的机器上网，会造成不便。

所以该方案存在如下缺点：

（1）在 SET 协议标准下，不仅全球商户需要在认证机构进行认证，消费者也必须从认证机构获取电子证书。这给消费者带来了很大的不便。

（2）在 SET 协议标准下，不但商户要在其服务器上安装复杂的软件，而且消费者要在其 PC 上安装过于复杂的软件以进行电子商务和诸存电子证书。消费者因此望而却步。

（3）由于消费者电子证书安装在固定的 PC 机上，因此持卡人电子商务交易必须通过固定 PC 机进行，这大大限制了消费者电子商务的进行。

（4）由于电子证书安装在消费者网络接入设备上，这使得那些无法安装电子证书的网络接入设备如移动电话、PDA 等则无法进行电子商务。

（5）对于小额交易来说，消费者为完成交易而花费的成本甚至高

于所交易的金额，因此消费者在进行小额交易时完全没有动力使用 SET 安全协议。

3. 3-D SET 标准

3-D SET 标准是在 SET 的基础上推出的；改进之处有：

1）在 3D SET 下，不要求消费者在其 PC 机（或其它 Internet 接入设备）上安装复杂的软件以进行电子商务交易和储存电子证书。

2）在 3D SET 环境下，由于消费者不需要在 PC 机上储存电子证书，消费者可以通过任何网络接入设备进行电子商务并能从发卡机构处获得认证，而不仅仅局限于 PC。

但该 3-D SET 标准仍然存在下列缺陷：

1）和其它证书认证方法一样，它有其缺陷，即消费者必须持有其所拥有的所有银行卡的发卡机构的电子证书。由于消费者一般手头持有不止一张银行卡，要申请这些卡的各自发卡机构的电子证书，对普通消费者来说，显得十分麻烦。

2）由于消费者可以从任何网络接入设备进行电子商务，证书认证相对于简单的密码认证来说，就显得多余且麻烦了。

3）3D SET 标准与 SSL 协议不相兼容。由于 SSL 已被大众广泛接受，并普及到现实的电子商务网上支付数据传输当中，故 SSL 往往就成为电子商务的默认设置，因此在推广上有很大的局限。

4. Visa 3D Secure 安全认证体系

2001 年，Visa 国际卡组织推出 Visa 3D Secure 安全认证体系。

Visa 的 3D 并不是一个支付和认证的方法，也不是一个单纯的技术方案，Visa 3D Secure 实际上是一整套的网上安全支付认证体系。在这个支付认证体系中，交易的进行要对持卡人（发卡机构对持卡人）、商户（收单机构对商户）进行认证。

3D Secure 中的 3D 是英文 3 Domains 的缩写，即 3 个域的意思。这 3 个域分别是：发卡机构域（包括持卡人和发卡机构）、收单机构域（包括商户和收单机构）和中间组织域（Visa）。

其明显的优点在于：

1）对持卡人参与电子商务的硬软件要求最小化。持卡人只须能够使用一台能够上网的安装有浏览器（IE）的电脑即可；

2）相对于 SET 标准来说，Visa 3D Secure 认证体系只要商户对持卡人进行认证，而不需要持卡人对商户进行认证，商户的身份由 Visa 认可的 CA 对商户颁发证书进行证书认证；

3）采用对持卡人密码认证取代了证书认证，大大简化了认证程序。

缺点是：

1) 由于 3D Secure 认证体系采取先认证后授权中心型的网络架构，每笔交易过程要多几道交易流程，因此交易过程要多花费时间。
2) 持卡人必须填写所有详细交易信息；在持卡人到多个商户处进行多笔交易时，每笔交易都要进行一次密码输入。
3) 在该种认证方案下，发卡机构都要安装复杂的支持网上交易的服务器，以进行持卡人注册和认证等服务。

Visa 3D Secure 认证体系采取了中心化的网络架构，所有认证者需要 Visa Directory 的参与；从交易流程来看，Visa Direcrory 并不是一个有效率的技术方案，它迟滞了信息流，增加了信息传递的环节，最终影响着整个交易流程，还可能成为黑客攻击的目标；该认证方式都在技术层面上也使用了 SSL 的文件加密传输协议。由于持卡人的认证过程和授权过程是分开的。从认证过程过看，欺诈做案的商户会容易地控制 MPI 以非法获取持卡人信息。为了避免出现上述的商户欺诈行为，3D Secure 要求商户要取得 Visa 认可的 CA 的数字证书认证，这自然增加了 3D Secure 认证体系的安全性，但同时也增加了其运行的复杂性。

综上所述，传统或现有的网上支付安全体系的缺陷可以归纳如下：

SSL

SSL 实现了数据点对点的安全传输，保证了数据传输的完整性和保密性，但 SSL 无法实现对交易主体的认证，没有任何方法证明交易主体

身份的合法性，因此单纯 SSL 协议无法保障网上支付的顺利进行。

但 SSL 本身却是一种成熟的技术，得到了广泛的应用，无论是紧随其后出现的 SET、3D SET 技术，还是国际卡组织最近推出的 3D Secure 认证体系，其技术内核都嵌入了 SSL 加密技术。

SET

Set 协议的最大缺陷在于其对证书认证方式的高度依赖，最主要的失败之处在于对持卡人证书认证方式。由于持卡人分散性、流动性并且数量众多，因而理论上虽然也可以做到对持卡人发证书的方式把持卡人固定下来并在电子商务时进行身份认证，但实践上却是行不通的。

3D SET

由于 3D SET 认证继承了 SET 对持卡人实行证书认证的失败，因而 3D SET 整体上也是一种失败的认证体系；而且 3D SET 认证体系另外一处明显的缺陷是与 SSL 协议的不相兼容性。

3D Secure

3D Secure 认证体系的表面完善性背后有一个盲点，就是当卡号和密码等重要信息同时被不法之人获知时，3D Secure 认证体系的密码验证机制就失效了。另外，持卡人、商户、发卡机构以及收单机构四者或全部或部分必须进行技术改造与升级才能支持该认证体系的运作。

发明内容

本发明的目的在于提供一种安全的网上支付认证办法，建立一个安全的网上支付系统，既要足够安全，客户的重要信息如信用卡号码等银行资料避免在网络中被他人获取，同时处理效率要高，成本要低；而且认证方法有便利，尤其是客户和商户要在交易活动中感到方便。

分析以上现有技术，我们可以得到如下一些结论：

1. SSL 信息加密传输协议是一套成熟的技术，仍可利用；
2. 持卡人证书认证方案理论上完美，实际操作性差；
3. 数据加密传输代替透明传输是一种有效的安全措施，持卡人信息能避过商户与收单机构则将更加安全；

4. 对商户、收单机构和发卡机构进行证书认证，但要客观合理。

本发明采用了如下的技术方案，提供了一种安全的网上支付认证办法，建立了一个安全的网上支付系统。

一种网上支付系统，包括如下组成部分：

客户，即消费者，需要从其帐户中支付一定数量货币的一方，

客户支付帐户银行或其代理行，即可以确认帐户信息和执行扣款支付的一方，也称付款人帐户开户银行 ，

商户，即服务或商品提供者，应该收取款项的一方，

商户收款帐户银行或其代理行，也称收款方帐户开户银行，

支付平台，是负责处理来自网上的支付信息，并且认证客户和商户身份，确认交易真实有效的一个的处理系统，

客户、商户和支付平台通过互联网连接，在支付平台的处理系统确认交易的合法性之后，支付平台发出支付请求，并在支付完成后将支付信息通知交易双方，即客户和商户，

支付平台一端联系客户和商户，在互联网上确认客户身份与商户身份，网上对客户身份认证是密码认证，对商户身份认证是证书认证，并确认交易与交易金额；一端联系支付帐户银行和收款银行，传送支付请求与扣款信息，

为了保证交易安全，避免他们通过网络非法截取交易信息以及相关的身份信息、银行资料信息等，在支付平台与客户之间还设有客户身份辅助认证系统，该辅助认证系统连接客户与支付平台，并且是非互联网连接方式，支付平台在互联网上用密码初步确认客户身份并收到支付请求后，生成一个授权码，并通过客户身份辅助认证系统传送该授权码给客户，客户在收到该授权码以后，在支付平台的相应页面上输入该授权码，支付平台在核实授权码无误后，最终确认客户身份通过验证，发送支付信息，并从银行获得返回的处理信息，并将该处理信息转达给客户与商户。

所述的客户身份辅助认证系统包括一个客户终端和一个转接系统，

该客户终端在支付平台中有初始信息登记，该转接系统连接支付平台与客户终端，从支付平台接收信息并传送到客户终端。

所述的转接系统从支付平台接收的信息，包括授权码和交易信息。

所述的授权码是动态生成并且是有时效的，在时效范围以内输入到支付平台的相应页面，该授权码才能被认为是正确的，超出时间范围则被判断为无效的授权码。

所述的客户身份辅助认证系统的客户终端是专用设备，该专用设备在支付平台中有初始信息登记。

所述的客户终端可以是单独设置的由该支付平台提供的专用设备，只要是符合该支付平台标准的设备，也可以是由该支付平台提供的专用转接卡设置在个人或家庭常见电子或电器设备中形成，如在机顶盒、遥控器中加上专用转接卡等。

所述的客户身份辅助认证系统的客户终端当然也可以是非专用设备，如电话、手机、BP 机、PDA 等，该非专用设备作为客户终端使用前需要到支付平台或其指定地方进行初始信息登记。

所述的客户终端在该支付平台的初始信息登记可以是一个或多个客户终端的信息。所述的接收授权码的客户终端可以不是该支付平台中有初始信息登记的客户终端。

在该网上支付系统系统在支付平台和银行之间还设有银行信息处理系统，该银行信息处理系统连接支付平台、付款人帐户开户银行和收款方帐户开户银，支付平台发送支付请求给该银行信息处理系统，确认付款人帐户是否可以完成支付，并从该系统获得支付请求的处理结果，扣款成功或拒绝支付。

所述的支付平台和银行信息处理系统，是由不同机构或同一机构提供的网络平台

所述的银行信息处理系统，可以是由付款人帐户开户银行提供的网络平台或者是由收款方开户银行或其代理行提供的网络平台。

所述的支付平台和银行信息处理系统，也可以是由与交易无关的第三方提供的网络平台。

采用了本发明的网上支付系统的网上支付认证方法，包括对网上交易的双方，即客户和商户进行身份认证并确认其交易和交易金额，除了对商户身份进行证书认证和客户身份进行密码认证，还对客户身份还进行动态的辅助认证。

这种网上支付认证方法，包含如下步骤：

1. 客户网上浏览，发出交易请求，
2. 商户接收交易请求，
3. 客户发出支付请求，转入支付平台界面，
4. 支付平台要求客户在互联网上输入密码进行客户身份认证，并核实该密码，
5. 若密码不正确，则拒绝该交易请求，
6. 若密码正确，则动态生成授权码，
7. 支付平台通过客户身份辅助认证系统传送该授权码给客户，
8. 客户在收到该授权码以后，在支付平台的相应页面上输入该授权码，
9. 支付平台在核实授权码无误后，确认客户身份通过验证，发送支付请求，

该客户身份辅助认证系统传送授权码给客户系通过非互联网途径传送。

如果选择用手机作为客户终端、短信平台作为辅助认证系统的转接系统，则这种网上支付认证方法，包含如下步骤：

1. 客户在商户网站选择商品并形成订单；
2. 客户选择身份辅助认证方式为短信认证方式，
3. 客户进入到网上支付系统的支付平台界面，根据界面提示输入手机号码及约定的网上支付密码；
4. 支付平台收到客户信息后对手机号及网上支付密码进行判断，若该手机信息已经有初始信息并且密码准确，则动态生成一个授权码；

5. 支付平台将该授权码发往短信中心；

6. 短信中心将收到的授权码发到客户手机上；

7. 客户收到短信，根据提示在支付网页上输入授权码；

8. 支付平台对授权码进行校验无误后，视为客户身份认证通过，进行下一步的支付程序。

授权码是动态生成的同时还指定了该授权码的有效时间，必须在指定的时间范围内输入正确的授权码。

支付平台通过客户身份辅助认证系统传送该授权码给客户，系传送到客户终端上，该客户终端可以是支付平台上登记有初始信息的客户终端，也可以是由客户选择或指定的。

转接系统从支付平台接收的信息，可以包括授权码和交易信息。同样的，其发送给客户的信息也可以包括授权码和交易信息。

转接系统可以使用已有的设施，如电信网络、有线电视网络等。

所述的客户身份辅助认证系统的客户终端可以是专用设备，该专用设备可以单独设置，也可以设置在其他电子或电器设备中，如机顶盒、遥控器等，所述的客户身份辅助认证系统的客户终端也可以是非专用设备，如电话、手机、PDA、非专用设备作为客户终端使用前需要到支付平台或其指定地方进行初始化数据登记。

具体实施方式

为了更好地详细说明本发明的内容，首先需要定义如下在网上支付系统中使用的名词或术语：

客户——消费者，即电子商务中的购物方，银行卡的持卡人，网上支付的发起方。

支付平台（Payment Gateway）——是位于互联网和银行内部业务处理系统之间的一个信息转换系统，它专门负责处理来自 Internet 上的支付信息。它可以是公共平台，也可以是某个转接系统提供的专用平台，或者是某个银行提供的平台，或者是某个代理银行提供的平台。

发卡银行——发卡银行对持卡客户通过支付平台发来的本行银行

卡支付信息进行验证、账务处理并返回处理结果。包括收款方帐户开户银行或付款人帐户开户银行。既可以是狭义的银行卡的发卡银行，又可以是广义的任何形式的帐户的开户银行。

网上商户——在互联网上提供商品或服务并接受银行卡支付方式的电子商务企业；网上商户可直接与发卡方支付平台连接，也可通过支付中介与发卡方网关连接。

支付中介——为电子商务企业提供网上收款服务的专业机构，与多个发卡银行的支付平台建立连接，支持多种银行卡支付方案，并代理商户与发卡银行进行结算。如无支付中介，商户必须与多家发卡银行建立连接才能支持多种银行卡的支付。在本发明中，收款方帐户开户银行或付款人帐户开户银行的功能可以由支付中介来替代。

网上商户清算行——网上商户的开户银行，为商户提供资金结算服务。

CA 认证机构（Certification Authority）——CA 是为了解决电子商务活动中交易参与各方身份、资信的认定，维护交易安全，从根本上保障电子商务交易活动顺利进行而设立的权威仲裁机构。

网上支付主要环节如下：

客户通过网络向网上商户提交订单，确认支付后，即进入网上支付过程，主要包括 4 个环节。

i. 客户认证——由于大部分网上支付是无卡、无磁条交易，如何解决对客户身份的认证是网上支付的重要环节。

ii. 订单确认——网上支付必要环节，其中包含对商户的认证。

iii. 发卡方扣帐——确定客户和订单后，发卡方即可进行扣帐处理。发卡方完成扣帐，标志着网上支付成功，商户即可向客户提供商品和服务。

iv. 商户清算——商户清算行向商户划拨资金。

下面详细描述本发明的系统构成。

一种网上支付系统，包括如下组成部分：

客户，即消费者，需要从其帐户中支付一定数量货币的一方，

客户支付帐户银行或其代理行，即可以确认帐户信息和执行扣款支付的一方，也称付款人帐户开户银行 ，

商户，即服务或商品提供者，应该收取款项的一方，

商户收款帐户银行或其代理行，也称收款方帐户开户银行，

支付平台，是负责处理来自网上的支付信息，并且认证客户和商户身份，确认交易真实有效的一个的处理系统，

客户、商户和支付平台通过互联网连接，在支付平台的处理系统确认交易的合法性之后，支付平台发出支付请求，并在支付完成后将支付信息通知交易双方，即客户和商户，

支付平台一端联系客户和商户，在互联网上确认客户身份与商户身份，网上对客户身份认证是密码认证，对商户身份认证是证书认证，并确认交易与交易金额；一端联系支付帐户银行和收款银行，传送支付请求与扣款信息，

为了保证交易安全，避免他们通过网络非法截取交易信息以及相关的身份信息、银行资料信息等，在支付平台与客户之间还设有客户身份辅助认证系统，该辅助认证系统连接客户与支付平台，并且是非互联网连接方式。所述的客户身份辅助认证系统包括一个客户终端和一个转接系统，该客户终端在支付平台中有初始信息登记，该转接系统连接支付平台与客户终端，从支付平台接收信息并传送到客户终端。

客户在进行网上交易之前，需要首先在支付平台中有初始信息登记，即首先有客户身份与客户帐户之间的对应关系及其基本信息的登记、支付平台中还有其他数据库或记录方式存放的信息，例如，客户帐户与其开户行的对应信息等；客户在网上交易时，可以是其真实身份，或者是对应于其真实身份的网上交易客户身份。支付平台在处理交易请求时，首先核实网上输入得客户身份是否在该支付平台中有登记，若在网上输入的客户身份正确，即视为其通过了客户身份的初步确认，其网上交易行为开始。支付平台也可以在核实输入的客户身份正确以后，按照初始信息登记中的约定，要求客户输入网上交易密码，以确认客户身份通过初步认证。客户或者通过专用客户终端，即由支付平台或其认同

的机构给出对应于某个专用客户终端的网上支付密码；或者是由客户到支付平台指定地方进行初始化信息登记时约定一个网上支付密码。该网上支付密码是可以由客户修改的。

当客户在支付平台中登记了初始信息以后，就可以非常安全方便地开始其网上交易活动了。如果客户设置了网上交易密码，则在进行客户身份认定时，首先使用该密码作初步的身份认定。这样就避免了在网上交易时在互联网的界面上输入信用卡号码或对应的信用卡密码。也可以说是客户的真实身份得到了“屏蔽”，客户的真实的银行资料得到了保护。

支付平台在互联网上用密码初步确认客户身份并收到支付请求后，生成一个授权码，并通过客户身份辅助认证系统传送该授权码给客户，客户在收到该授权码以后，在支付平台的相应页面上输入该授权码，支付平台在核实授权码无误后，最终确认客户身份通过验证，发送支付信息，并从银行获得返回的处理信息，并将该处理信息转达给客户与商户。

其中上述的授权码是动态生成的，其生成规则由支付平台实时调整，在支付平台中，该规则本身也是动态变化的，有一定的时效性。授权码根据需要也可以被设定一定的有效时间范围。这样，授权码和其生成规则均是动态变化且设定时效的，动态码的传输途径是非互联网途径，动态码的接收终端是他人不易获得的，所以保证了网上交易的安全。

上述系统中的接收授权码的客户终端可以是指定的，例如一个客户在支付平台的初始信息中可以登记若干条记录，在交易过程中，可以约定将授权码发送到某个客户终端上，使得他人窃取授权码的可能性降到最低。

这种网上支付认证方法，包含如下步骤：

1. 客户网上浏览，发出交易请求，
2. 商户接收交易请求，
3. 客户发出支付请求，转入支付平台界面，
4. 支付平台要求客户在互联网上输入密码进行客户身份认证，并核实该密码，

5. 若密码不正确，则拒绝该交易请求，
6. 若密码正确，则动态生成授权码，
7. 支付平台通过客户身份辅助认证系统传送该授权码给客户，
8. 客户在收到该授权码以后，在支付平台的相应页面上输入该授权码，
9. 支付平台在核实授权码无误后，确认客户身份通过验证，发送支付请求，

该客户身份辅助认证系统传送授权码给客户系通过非互联网途径传送。

如果选择用手机作为客户终端、短信平台作为辅助认证系统的转接系统，则这种网上支付认证方法，包含如下步骤：

1. 客户在商户网站选择商品并形成订单；
2. 客户选择身份辅助认证方式为短信认证方式，
3. 客户进入到网上支付系统的支付平台界面，根据界面提示输入手机号码及约定的网上支付密码；
4. 支付平台收到客户信息后对手机号及网上支付密码进行判断，若该手机信息已经有初始信息并且密码准确，则动态生成一个授权码；
5. 支付平台将该授权码发往短信中心；
6. 短信中心将收到的授权码发到客户手机上；
7. 客户收到短信，根据提示在支付网页上输入授权码；
8. 支付平台对授权码进行校验无误后，视为客户身份认证通过，进行下一步的支付程序。

授权码是动态生成的同时还指定了该授权码的有效时间，必须在指定的时间范围内输入正确的授权码。

支付平台通过客户身份辅助认证系统传送该授权码给客户，系传送到客户终端上，该客户终端可以是支付平台上登记有初始信息的客户终端，也可以是由客户选择或指定的。例如，一般是以手机作为接收动态授权码的客户终端，但也可以选择返回到一个 BP 机上

或者是其他的设备上。

这样，网上交易时，根据初始信息登记，以手机号码作为客户的身份码，避免了在网络上输入身份证号码或银行卡号码，安全性得到了保障；同时因为采用了密码认证方式，灵活而方便，符合广大客户的消费需求。

转接系统从支付平台接收的信息，可以包括授权码和交易信息。同样的，其发送给客户的信息也可以包括授权码和交易信息。并且该包含授权码的短消息的发送和接收方式是采用转接系统的一般加密方式或再次加密方式进行的。

转接系统可以使用已有的设施，如电信网络、有线电视网络等。

上述实施例中本发明的网上支付系统的结构是这样的：由两个物理平台组成，一个是互联网平台，一个是电信短信息平台；

本系统包括以下各部分：客户（即持卡人，消费者），网上商户，支付平台，银行信息处理系统，付款人帐户开户银行或其受理行；短信中心，短信接收客户终端——手机。

其中客户、网上商户、支付平台、银行信息处理系统、付款人和收款方帐户开户银行通过互联网连接，但客户和商户只能访问或联系支付平台，不能和银行信息处理系统连接；银行信息处理系统连接支付平台和付款人帐户开户银行和收款方帐户开户银行。支付平台发送支付请求给银行信息处理系统，并获得返回的处理结果；在本实施例中支付平台不直接连接到银行。

所述的客户身份辅助认证系统的客户终端可以是专用设备，该专用设备可以单独设置，也可以设置在其他电子或电器设备中，如机顶盒、遥控器等，所述的客户身份辅助认证系统的客户终端也可以是非专用设备，如电话、手机、BP 机、PDA、非专用设备作为客户终端使用前需要到支付平台或其指定地方进行初始化数据登记。

在上述的辅助认证系统中，采用电信的短信息平台作为转接系统，对商户进行证书认证，对客户进行 2 次身份认证，一次是密码认证，一次是动态的授权码认证。

本发明的网上支付系统的业务流程可以是这样的：

业务流程 1

1. 客户在商户网站选择商品并形成订单，提交支付。
2. 客户进入到网上支付系统的支付网页，选择付费方式为手机支付，页面提示客户输入手机号码及 网上支付密码，并发送至支付平台；
3. 支付平台收到客户信息后对手机号及 网上支付密码进行判断，若该客户手机已经有初始信息登记，则产生一个无法被预测的授权码，连同付款金额，编辑成一则短消息；
4. 支付平台将短信息发往短信中心，
5. 短信中心将短消息转发至客户手机上。
6. 客户收到短信息，确定付款金额，根据提示在支付网页上输入授权码。
7. 支付平台对授权码进行校验，通过校验后将信息发往付款人帐户开户行的交易处理系统。
8. 交易处理系统执行扣款请求，银行扣款完成后返回处理结果给支付平台，
9. 支付平台返回处理信息给商户和客户。

业务流程 2

1. 持卡人在商户网站选择商品并形成订单；
2. 客户选择附费方式为银行卡支付短信认证方式时，进入到网上支付系统的支付网页，客户根据界面提示输入手机号码及网上支付密码；
3. 支付平台收到客户信息后对手机号及网上支付密码进行判断，若该客户手机已经定制，则产生一个授权码；
4. 支付平台将该授权码发往短信中心；
5. 短信中心将收到的授权码和支付金额发到客户手机上；
6. 客户收到短信，确认支付金额后，根据提示在支付网页上输入手机号码，授权码；

7. 支付平台对授权码进行校验无误后，将扣款信息发往银行信息处理系统；
8. 银行信息处理系统向付款人帐户开户银行发送扣款请求；
9. 付款人帐户开户银行扣款完成后向银行信息处理系统返回处理结果；
10. 银行信息处理系统将处理结果返回给支付平台；
11. 支付平台记录交易结果并将交易结果转发给商户，商户收到支付成功信息后，向持卡人提供相应的商品或服务。

采用上述认证方式有如下优点：

网上支付手机短信息认证模式有效地避免了卡号和密码均被获知情况下非法网上交易的进行，有效地保护了持卡人利益。由于持卡人要经过密码和手机短消息随机授权码的双重认证，保证了持卡人的身份真实性。

手机短消息认证模式下网上支付各参与方无须经过大规模的技术升级改造，因此从经济性来说，这种认证模式简单易行，成本较低。

在网上支付手机短消息认证模式下一方面仍然在技术层面上利用了 SSL 加密技术，同时有效避免了持卡人证书认证的弊端，也避免了持卡人保密信息被商户甚至收单机构获知的可能性。

本发明解决了网上支付的安全问题：从数据保密性和完整性来看，短消息认证模式应用有效的数据传输加密技术，数据流的关键信息有效地回避了商户，也避免了被网络侵入者截获并非法使用；

从交易主体的真实性来说，手机短消息认证模式下对持卡人进行了双重认证，比 3D Secure 认证体系下单纯的密码认证更具安全性。

无需客户输入卡号、ATM 取款密码和信用卡有效期，避免了敏感信息通过网络传输被黑客截获的危险。

客户通过输入手机号码和网上支付专用业务密码进行初步身份验证，再输入手机动态接收的对每笔网上支付唯一产生的动态授权码进行二次验证，即使初次验证信息被截获，二次验证信息由网上支付系统唯一产生，通过短信平台发送至客户手机，不通过网络途径，理论上说，

这种认证模式采用的双渠道安全方案较单一渠道安全方案的安全性更高，难以攻破，将大大增强网上支付的安全性。

这种密码验证方式，相比证书验证方式，具有灵活、易被接受的特点。

因为手机已成为非常大众化的通讯工具，所以非常便利，而且操作步骤简单明确，在支付使用不同银行卡时，面对的是统一的支付界面，不再需要理解各银行不同的规则，掌握不同的操作。同时也低成本认证。

客户信息的初始化登记，申请开通或取消网上支付功能：

客户可以向其发卡银行申请开通认证模式的网上支付，确定银行卡对应的移动电话号码；取消也相同。系统能够支持一个手机号码对多个银行卡号。

付款人帐户开户银行将开通或取消信息实时发送到网上支付系统的支付平台，该系统保存该信息，作为验证的依据，并向持卡人发送确认信息。

客户也可以设置每次支付限额和每天支付限额。

客户到付款人帐户开户银行申请开通或取消可以有以下方式：

1）由客户到银行柜台前办理；

2）通过网络直接办理注册；

3）通过专用设备如 POS 等终端设备办理。

客户在初始化信息登记时确定网上身份码，该码可以是手机号码，帐户号码、支付平台赋予的号码或者是客户自行选择的码。在网上交易时，可以在通过密码认证后，选择返回的客户终端。

上述表述仅为更好的表述和理解本发明的技术方案，而非用来限制本发明的实施方案。本领域技术人员可以对发明有替代的实施方式，但只要不超出本技术方案记载的内容，依然落入本发明范围以内。